Avira Mac Security

mit AMC-Unterstützung

Kurzanleitung

AVIRA

Inhaltsverzeichnis

1. Einführung 3
1.1 Merkmale 3
1.2 Systemanforderungen 4

2. Installation 4
2.1 Installation mit dem Installationsassistenten 4
2.2 Installation über das Terminal 5
2.3 Installation über die Avira Management Console 5
2.3.1 Unsichtbare Installation mit der Avira Management Console 9
2.3.2 Anpassung bei aktivierter Firewall 10

3. Statusübersicht 12
3.1 Ihr Mac ist geschützt! 13
3.2 Ihr Mac ist nicht geschützt! 14

4. Planer 15
4.1 Planen von Prüfläufen und Updates 15
4.2 Planen von Prüfläufen 15
4.3 Planen von Updates 16

5. Quarantäne und Logs 17
5.1 Quarantäne 17
5.2 Logs 18

1. Einführung

Mit diesem neuen Mac-Produkt bringt Avira denselben hohen Sicherheitsstandard zur Mac OS X-Plattform, der bislang nur für Windows und Unix Betriebssysteme verfügbar war.

1.1 Merkmale

Ihr Avira Produkt wird als 64-Bit-Paket (.pkg) bereitgestellt und umfasst die folgenden Funktionen:

- Ereigniscenter zur Überwachung, Verwaltung und Steuerung des gesamten Programms
- Zentrale Konfiguration der Einstellungen
- Ereignisdatenbank (Logs)
- Echtzeitschutzscanner zur ständigen Überwachung sämtlicher Dateizugriffe
- Systemprüfung zur konfigurierbaren Suche nach allen bekannten Typen von Viren und Malware
- Integrierter Planer zur Planung von wiederkehrenden Aufgaben wie Updates oder Virenprüfungen
- Integriertes Quarantäne-Management zur Isolation und Behandlung verdächtiger Dateien
- Extrem hohe Viren- und Malware-Erkennungsrate durch innovative Scan-Technologie (Scan-Engine) einschließlich heuristischer Prüfverfahren.
  Während der Systemprüfung werden Dateien und Ordner auf Viren geprüft. Anschließend wird das Ergebnis in der grafischen Benutzeroberfläche angezeigt.
  Der Echtzeitschutz wird als Dämonprozess im Hintergrund ausgeführt, überwacht alle Dateizugriffsversuche und blockiert den Zugriff auf infizierte Dateien
- Erkennung aller gebräuchlichen Archivtypen, einschließlich Erkennung verschachtelter Archive und Smart-Extension-Erkennung

1.2 Systemanforderungen

- CPU: Intel Core 2 Duo 64-Bit oder besser (das Avira Produkt ist nicht auf den 32-Bit-Prozessoren Intel Core Solo/Intel Core Duo lauffähig)
- Mindestens 2 GB RAM
- Mindestens 200 MB freier Speicher auf der Festplatte
- Minimale Systemanforderungen: Version 10.6 oder höher
- Mac OS X Server wird nicht unterstützt
- Ggf. ein funktionsfähiger Internetzugang (siehe Installation)
- Adobe Reader um das Benutzerhandbuch, die Kurzanleitung und andere Supportdokumentationen lesen zu können (www.adobe.com)

2. Installation

Sie finden die aktuellste Version von Avira Mac Security im Download-Bereich auf der Avira Webseite.
Avira Mac Security ist als 64-Bit-Paket verfügbar.

► Laden Sie das Paket auf Ihren Mac herunter.

2.1 Installation mit dem Installationsassistenten

► Durch einen Doppelklick auf das Paketsymbol starten Sie den Installationsassistenten, der Sie Schritt für Schritt durch die Installation führt.

► Auf dem Willkommens-Bildschirm klicken Sie auf **Fortfahren.**

► Lesen Sie den Softwarelizenzvertrag. Avira Mac Security kann nur installiert werden, wenn Sie die Bedingungen des Endbenutzer-Lizenzvertrags (EULA) akzeptieren. Klicken Sie erneut auf **Fortfahren.**

► Daraufhin werden Sie im nächsten Dialogfenster gefragt, ob Sie den Softwarelizenzvertrag akzeptieren. Mit einem Klick auf **Ablehnen** bricht die Installation ab. Bei einem Klick auf **Akzeptieren** wird die Installation fortgesetzt.

- ► Auf dem nächsten Bildschirm wird der benötigte Speicherplatz für die Standardinstallation von Avira Mac Security auf Ihrer Festplatte angezeigt. Vergewissern Sie sich jedoch, dass Sie mindestens 200 MB Platz auf Ihrer Festplatte verfügbar haben, wie es in den Systemanforderungen angegeben ist.
  Klicken Sie auf die Schaltfläche **Installieren** um die Installation auszuführen.

- ► Das Betriebssystem wird Sie nach Ihrem Benutzernamen und Passwort fragen, um die Installation zu erlauben. Wenn Sie die Daten eingegeben haben, klicken Sie auf **OK.**

- ► Nach der erfolgreichen Installation klicken Sie auf die Schaltfläche **Schließen.**

2.2 Installation über das Terminal

- ► Loggen Sie sich nach dem herunterladen als „Root“ ein. Wählen Sie das Verzeichnis aus, wo Sie das Paket abgespeichert haben.
  Beispiel:
  ```
  cd /tmp
  ```

  Nun geben Sie folgendes ein:
  ```
  sudo installer -pkg ./avira_mac_security.pkg -target /
  ```

  Nach einer erfolgreichen Installation sollte folgende Meldung angezeigt werden:
  ```
  installer: The install was successful.
  ```

2.3 Installation über die Avira Management Console

Hinweis:

Um Avira Mac Security über die AMC verwalten zu können, benötigen Sie einen Lizenzschlüssel, der Ihnen auf Anfrage zugeschickt wird.

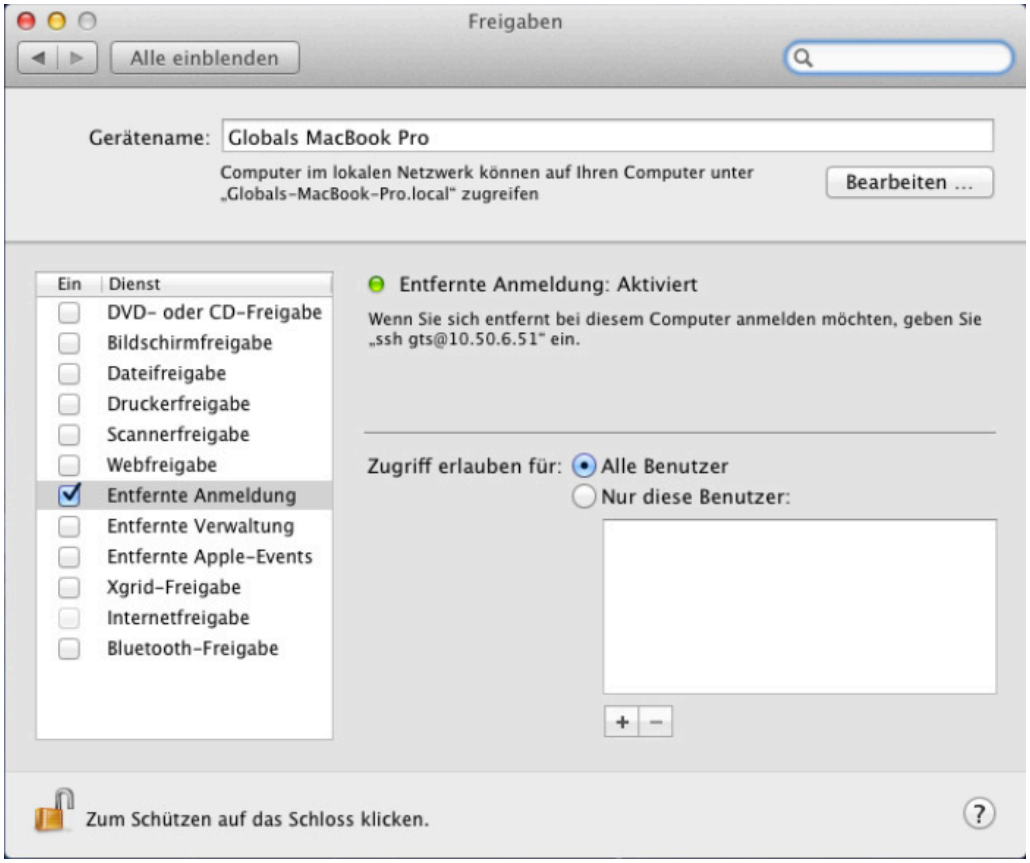
Weitere Details über den Umgang mit Software-Paketen innerhalb der AMC finden Sie in der Kurzanleitung zur Avira Management Console.

Wenn Sie einen oder mehrere Mac-Clients über die Avira Management Console verwalten möchten, müssen Sie die folgenden Schritte durchführen, damit Sie die Datei „avira_mac_security.pkg“ wie andere Pakete zum Bereich „Software Pakete“ im Frontend der AMC hinzufügen können:

- ► Aktivieren Sie SSH-Support, indem Sie das Terminal starten

- Öffnen Sie die Datei `/etc/sshd_config` (z.B. mit vim, vi oder nano) als „root“, aktivieren Sie den Parameter `PermitRootLogin` (`#` entfernen) und setzen diesen auf `yes`

- Aktivieren Sie die Entfernte Anmeldung auf Ihrem Mac, indem Sie *Systemeinstellungen* > *Freigaben* wählen (siehe Abb.).



Nach diesen Änderungen muss der Dienst SSH neu gestartet werden.
Hierzu genügt es entweder Ihren Mac neu zu starten oder folgende zwei Befehle in das Terminal einzugeben:

```
$ sudo launchctl stop com.openssh.sshd
$ sudo launchctl start com.openssh.sshd
```

Root-Passwort setzen

Für die erfolgreiche Installation von Avira Free Mac Security muss ggf. noch das Kennwort für den Benutzer „root“ gesetzt werden.
Dazu geben Sie folgenden Befehl im Terminal ein:

```
sudo passwd
```

Geben Sie anschließend das von Ihnen gewünschte Passwort ein.

Hosts anpassen

Wenn Sie die AMC auf Hostnamebasis installiert haben, müssen Sie dafür sorgen, dass bei einer Remote Installation des AMC Agents auch der Hostname Ihres AMC Servers aufgelöst werden kann.
Dazu tragen Sie mit einem Editor Ihrer Wahl die IP Adresse und Hostname in der `/etc/hosts` ein.

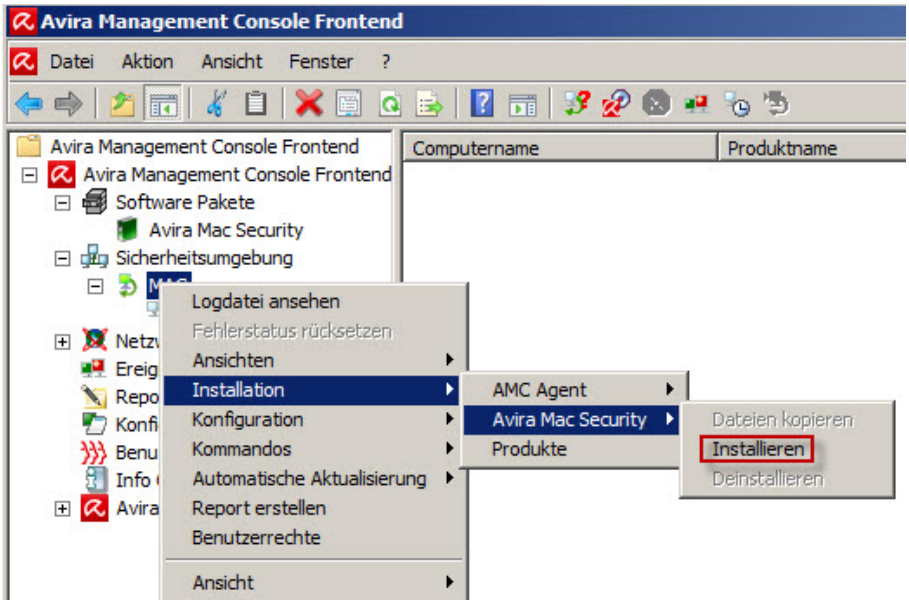
Beispiel:

```
192.168.2.1                AMCSERVER
```

Nach der Speicherung dieser Änderungen sollte nun eine Remoteinstallation des AMC Agents über die AMC möglich sein.

Wenn alles funktioniert, sehen Sie Ihren Mac mit einem grünen Rechner Symbol im AMC Frontend und Sie können das Avira Mac Security Paket auch auf Ihrem Mac installieren.

Wie bei anderen Softwarepaketen klicken Sie im AMC-Frontend innerhalb der Sicherheitsumgebung einfach mit der rechten Maustaste auf den Mac-Computer und wählen *Installation > Avira Mac Security > Installieren*



MAC Produkt wird nicht angezeigt obwohl installiert

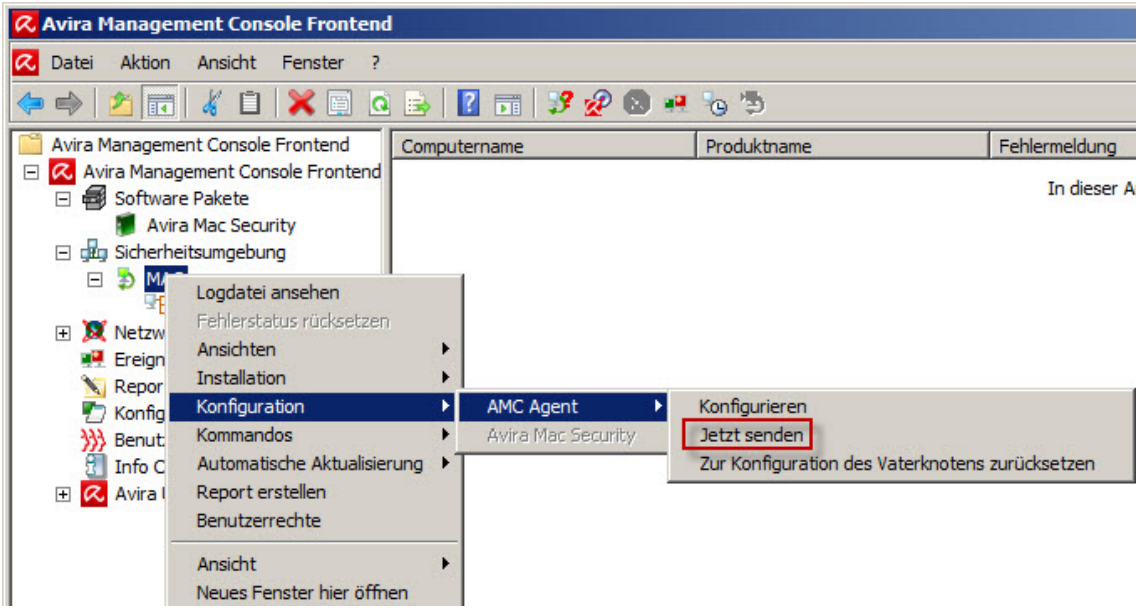
Falls es vorkommen sollte, dass Sie das Avira Mac Security Produkt schon installiert haben, nun den AMC-Agent nachziehen und das Produkt nicht angezeigt wird, können Sie dieses unter `/opt/avira/etc/agent.ini` eintragen.

Öffnen Sie diese Datei AGENT.INI (z.B. mit vim, vi oder nano) mit Schreibrechten und fügen Sie die folgenden Einträge ganz unten an.

```
[plugins]
osxsrv=/Applications/Avira.app/Contents/guard/agent/libosxsrv.dylib
```

Speichern Sie die Änderungen und starten Sie den AMC Agent neu.

Entweder Sie senden dem AMC Agent für Ihren Mac einfach nochmals eine Konfiguration (Über *Konfiguration* > *AMC Agent* > *Jetzt senden*)



oder Sie führen den folgenden Befehl im Terminal Ihres Macs aus:

```
sudo /opt/avira/agent/smcagent_restart.sh
```

2.3.1 Unsichtbare Installation mit der Avira Management Console

Sie können einen oder mehrere Mac-Clients z.B. über einen Rollout durch eine unsichtbare Installation von Avira Free Mac Security an das AMC anbinden.
Hierfür muss kein separater SSH Zugang konfiguriert werden. Benötigt wird lediglich ein Zugriff auf ein beliebiges Netzwerkshare, auf dem das Agent-Paket zur Verfügung gestellt wird.

Um die Installation zu starten, muss das Install-Skript aus dem Agent-Installationspaket mit den Zieldaten des AMC-Servers angegeben werden.
Außerdem ist ein `--inf`-Parameter sowie INF-Datei notwendig, um das Skript automatisiert laufen zu lassen.

Der Aufruf lautet dabei wie folgt:

```
./install --server_uri=http://<dnsname_or_IP-address> --dis-
play_name=<name> --update_uri=http:// <dnsname_or_IP-address>
--inf=./setup.inf
```

Die SETUP.INF enthält lediglich folgenden Eintrag:

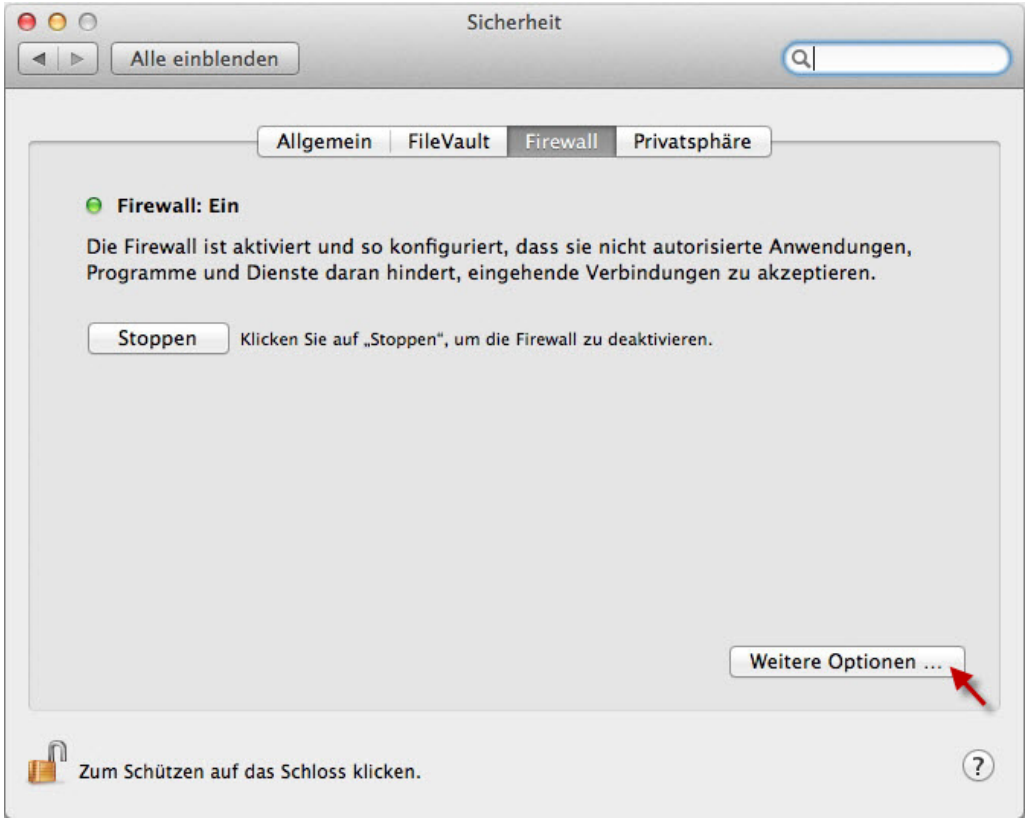
```
LICENSE_AGREEMENT=y
```

Nun startet das Setup und installiert sich automatisch auf dem System. Auch der Start und die Initialisierung (Anmeldung an der AMC) verlaufen selbstständig.

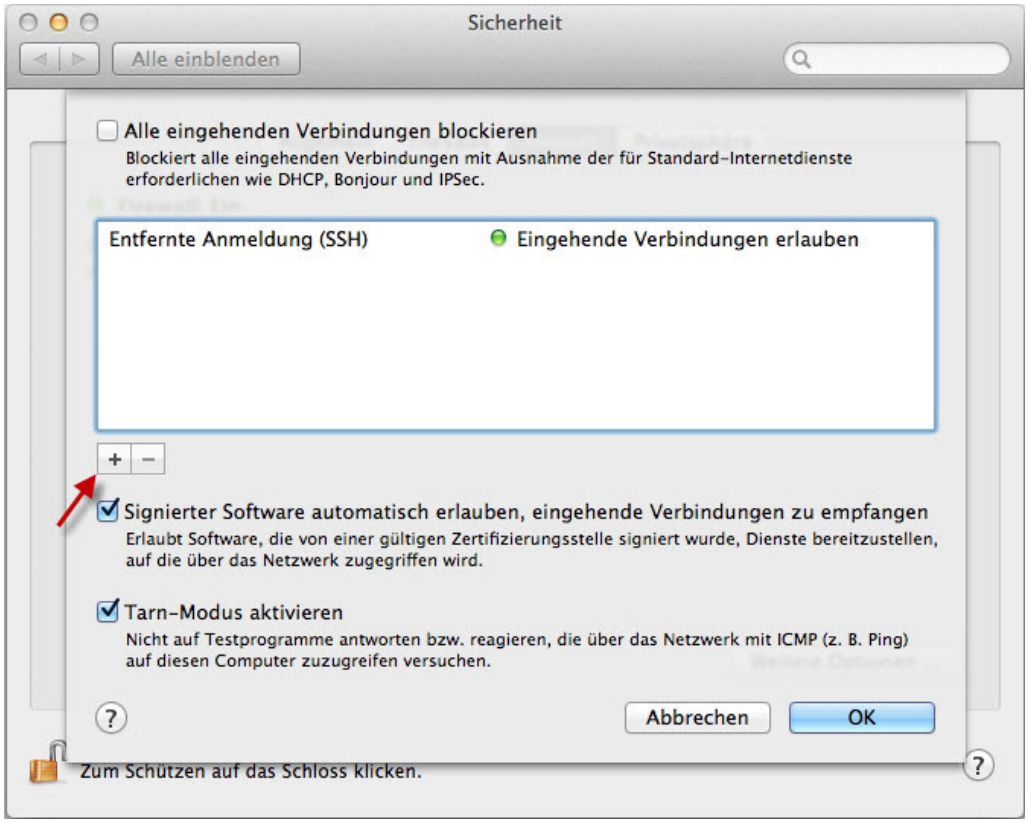
2.3.2 Anpassung bei aktivierter Firewall

Um eine störungsfreie Kommunikation zwischen dem Agent und der AMC zu gewährleisten, muss – sofern aktiviert – eine Firewall-Freigabe konfiguriert werden.

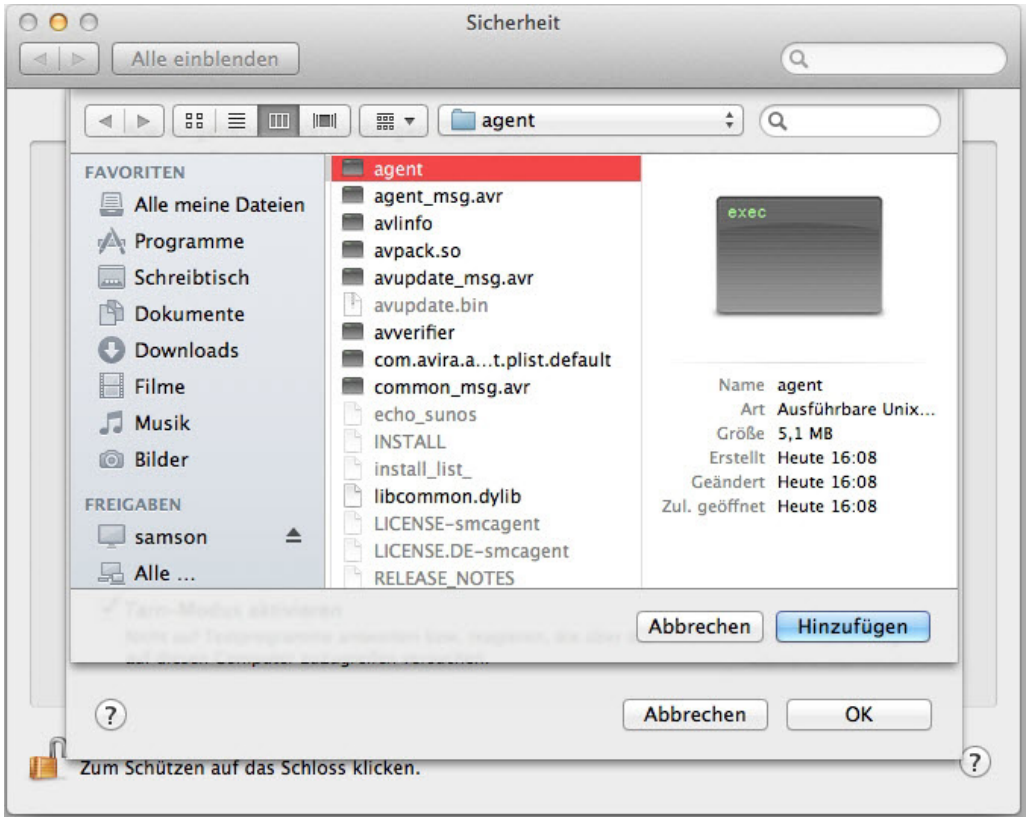
Öffnen Sie dazu die Firewall-Einstellungen unter *Systemsteuerung* > *Sicherheit* > *Firewall ...*



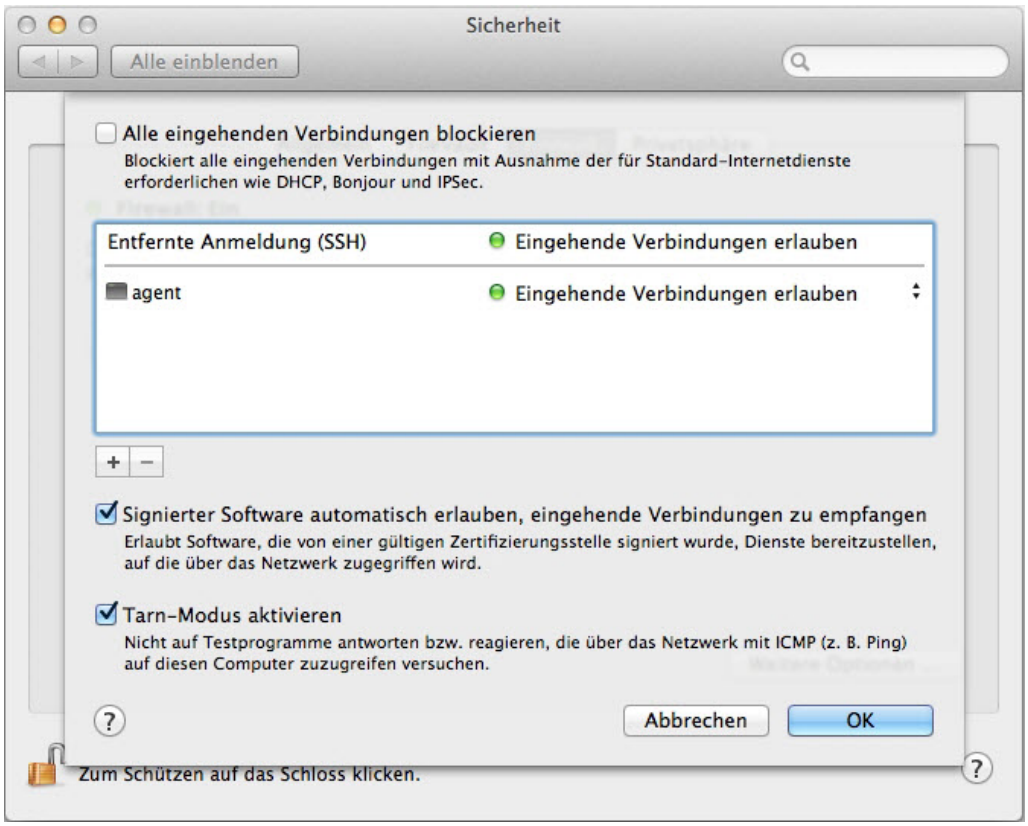
Wählen Sie nun „Weitere Optionen“ und entfernen Sie den Haken bei „Alle eingehenden Verbindungen blockieren“:


Sicherheit
Alle einblenden
Alle eingehenden Verbindungen blockieren
Blockiert alle eingehenden Verbindungen mit Ausnahme der für Standard-Internetdienste erforderlichen wie DHCP, Bonjour und IPSec.
Entfernte Anmeldung (SSH)
Eingehende Verbindungen erlauben
Signierter Software automatisch erlauben, eingehende Verbindungen zu empfangen
Erlaubt Software, die von einer gültigen Zertifizierungsstelle signiert wurde, Dienste bereitzustellen, auf die über das Netzwerk zugegriffen wird.
Tarn-Modus aktivieren
Nicht auf Testprogramme antworten bzw. reagieren, die über das Netzwerk mit ICMP (z. B. Ping) auf diesen Computer zuzugreifen versuchen.
Abbrechen
OK
Zum Schützen auf das Schloss klicken.

Fügen Sie nun über „+“ das Agent-Binary hinzu (zu finden unter `/opt/avira/agent/agent`):



Vergewissern Sie sich, dass nun alle eingehenden Verbindungen erlaubt sind:


Sicherheit
Alle einblenden
Alle eingehenden Verbindungen blockieren
Blockiert alle eingehenden Verbindungen mit Ausnahme der für Standard-Internetdienste erforderlichen wie DHCP, Bonjour und IPSec.
Entfernte Anmeldung (SSH)
Eingehende Verbindungen erlauben
agent
Eingehende Verbindungen erlauben
Signierter Software automatisch erlauben, eingehende Verbindungen zu empfangen
Erlaubt Software, die von einer gültigen Zertifizierungsstelle signiert wurde, Dienste bereitzustellen, auf die über das Netzwerk zugegriffen wird.
Tarn-Modus aktivieren
Nicht auf Testprogramme antworten bzw. reagieren, die über das Netzwerk mit ICMP (z. B. Ping) auf diesen Computer zuzugreifen versuchen.
Abbrechen
OK
Zum Schützen auf das Schloss klicken.

Klicken Sie zum Abschluss auf **OK**.

3. Statusübersicht

Das Fenster **Status** ist eine zentrale Plattform für Informationen, Ereignisse und Steuerungsaufgaben. Zusätzlich zu den Seitenleistenbereichen, die einzeln ausgewählt werden können, enthält es eine Reihe von Optionen, die auch über die Mac-Menüleiste zu erreichen sind.

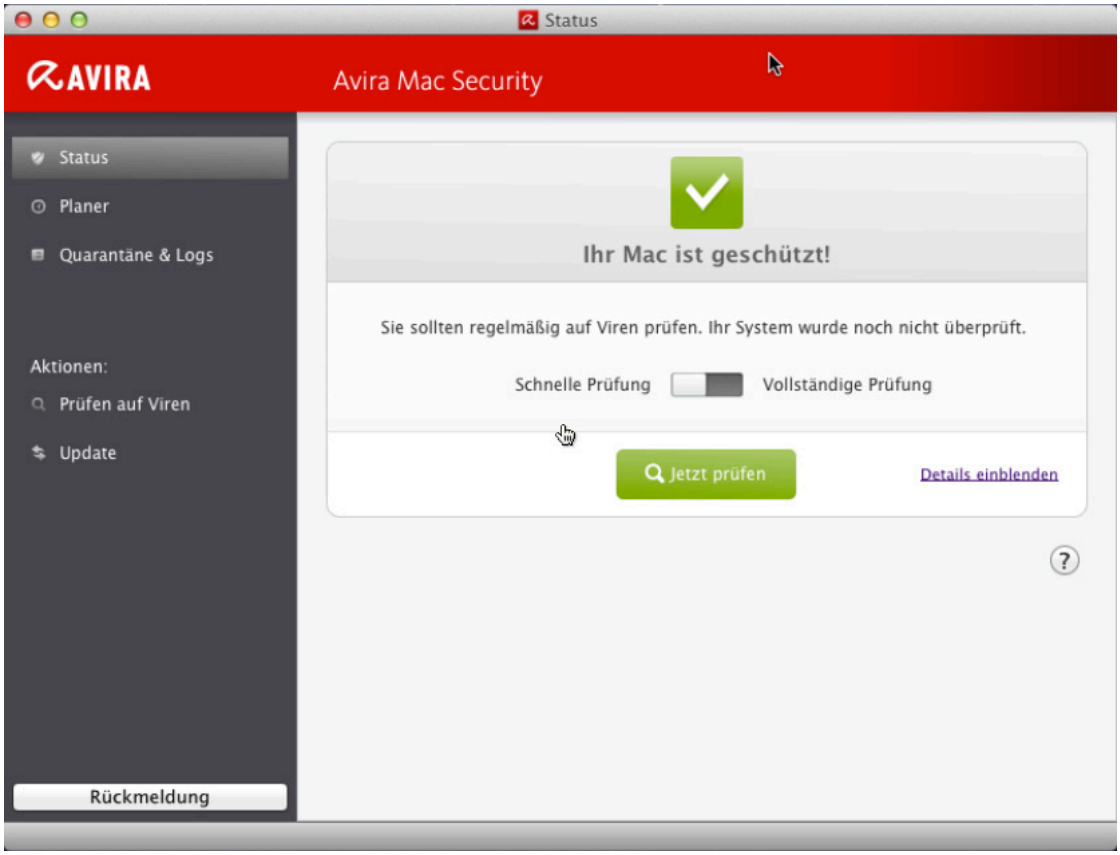
► Um das Fenster **Status** des Ereigniscenters zu öffnen, klicken Sie im Dock auf das Avira Logo. Alternativ dazu klicken Sie auf das Logo in der Menüleiste und wählen im Kontextmenü den Befehl **Avira öffnen.**

Im Fenster **Status** sehen Sie auf einen Blick, ob Ihr Mac geschützt ist. Außerdem wird angezeigt, wie viel Zeit seit der letzten Prüfung auf Malware verstrichen ist.

► Weitere Details zum Sicherheitsstatus erhalten Sie über den Link Details einblenden. Zusätzliche Information wird in den Bereichen der zwei Registerkarten *Status* und *Statistik* angezeigt. Klicken Sie auf den Link **Details ausblenden**, um die Registerkarten *Status* und *Statistik* auszublenden.

3.1 Ihr Mac ist geschützt!

Wenn die Meldung *Ihr Mac ist geschützt!* in Ihrem Statusfenster angezeigt wird, können Sie einen Scanprozess tatsächlich mit nur einem Klick starten.



► Klicken Sie auf den Schalter um zwischen **Schnelle Prüfung** und **Vollständige Prüfung** zu wählen.
Schalten Sie auf **Schnelle Prüfung** um eine Direktsuche in den anfälligsten Systembereichen durchzuführen. Wählen Sie **Vollständige Prüfung** für eine Direktsuche in allen Dateien, Verzeichnissen und Unterverzeichnissen.

► Um einen Scanprozess sofort auszulösen, klicken Sie auf die Schaltfläche **Jetzt prüfen**. Der Scanprozess wird mit einem blauen Fortschrittsbalken dargestellt. Das Ergebnisfenster wird die Dauer der Prüfung, die Anzahl der Dateien, die gescannt wurden und Informationen zu eventuell erkannter Malware anzeigen.

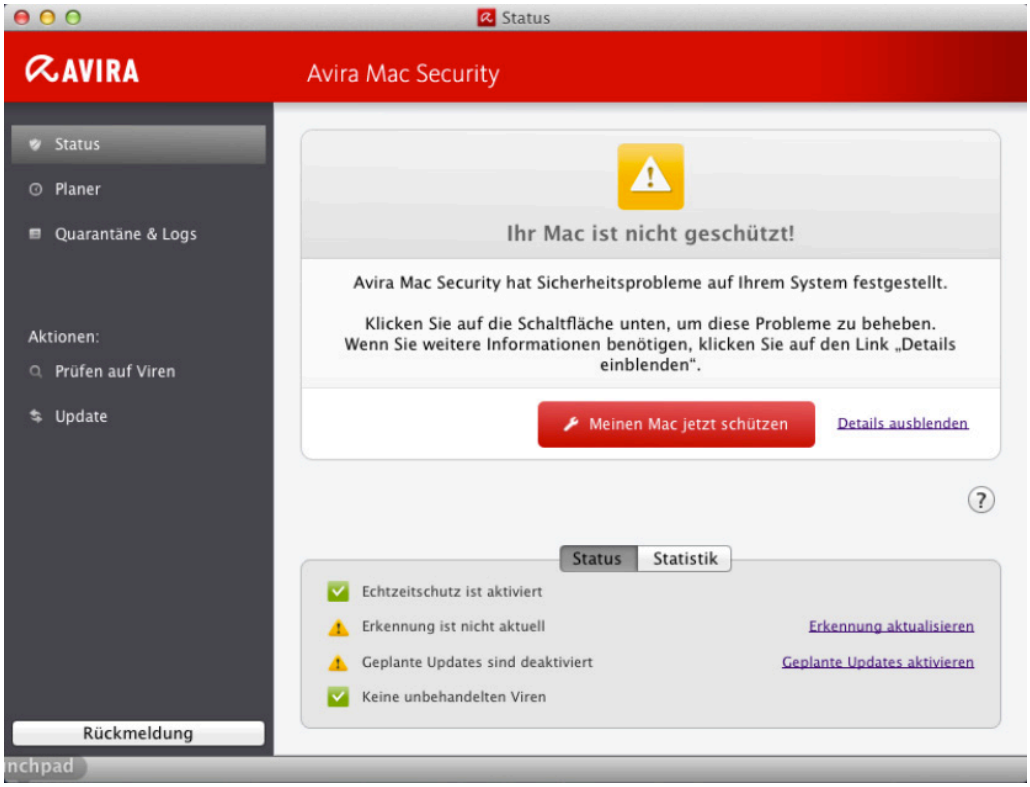
► Wenn Sie die Prüfung unterbrechen möchten, klicken Sie auf **Unterbrechen**.

► Wenn Sie den Prüflauf beenden möchten, klicken Sie auf **Abbrechen**.

Alternativ können Sie einen Prüflauf auch jederzeit starten, indem Sie im linken Bereich unter der Kategorie *Aktionen* **Prüfen auf Viren** anklicken.

3.2 Ihr Mac ist nicht geschützt!

Wenn jedoch die Meldung *Ihr Mac ist nicht geschützt!* in Ihrem Fenster **Status** angezeigt wird, können Sie dieses Problem einfach durch einen Klick auf die Schaltfläche **Meinen Mac jetzt schützen** beheben.



Wenn diese Probleme erfolgreich behoben wurden, wird Ihnen dies von Avira Mac Security so mitgeteilt.

In dem seltenen Fall, dass die Sicherheitsrisiken nach wie vor vorhanden sind, schlagen Sie bitte im Handbuch nach oder gehen zur Avira Support-Webseite.

Sie können natürlich wiederum auf den Link **Details einblenden** klicken, um zu sehen, welches Feature von Avira Mac Security ein Problem meldet.

4. Planer

4.1 Planen von Prüfläufen und Updates

Wählen Sie in der Seitenleiste die Option **Planer**, um regelmäßige Prüfungen und Aktualisierungen zu planen. Das Fenster **Planer** enthält zwei Registerkarten:

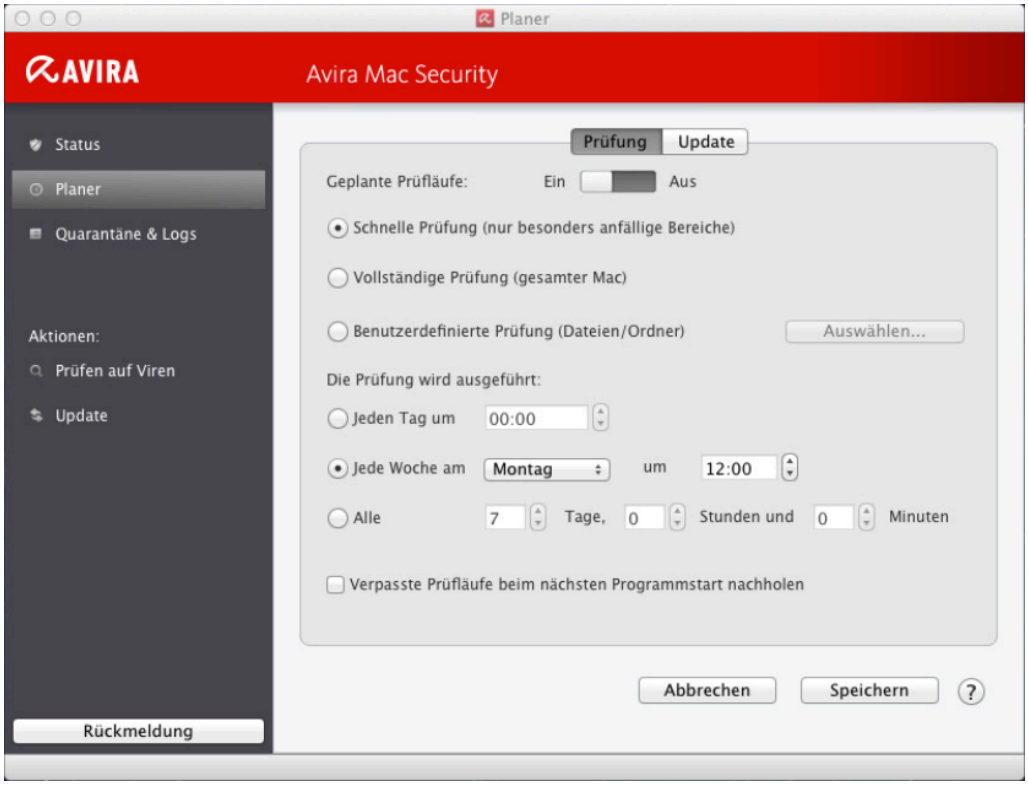
- Prüfen mit der Option zum Einstellen von **Geplante Prüfläufe** auf **Ein** oder **Aus**.
- Update mit der Option zum Einstellen von **Geplante Updates** auf **Ein** oder **Aus**.

► Klicken Sie auf eine Registerkarte um den betreffenden Bereich zu öffnen.

► Wählen Sie den gewünschten Vorgang aus und legen Sie den Zeitplan dafür fest.

4.2 Planen von Prüfläufen

Sie können über die Option **Planer** in der Seitenleiste zielgerichtete Prüfungen auf Viren und unerwünschte Programme planen. Wählen Sie *Planer* > *Prüfen* > *Geplante Prüfläufe* > *Ein*.



- ► Um die Option **Geplante Prüfläufe** zu aktivieren, bringen Sie den Standardschalter in die Stellung **Ein**.

- ► Wählen Sie die Option **Schnelle Prüfung** aus, wenn lediglich die anfälligsten Bereiche Ihres Systems geprüft werden sollen.

- ► Wählen Sie die Option **Vollständige Prüfung** aus, wenn Ihr gesamtes System auf Malware geprüft werden soll.

- ► Sie können auch die Option **Benutzerdefinierte Prüfung** auswählen und dann gezielt die Laufwerke und Ordner festlegen, die geprüft werden sollen.

4.3 Planen von Updates

Die Wirksamkeit einer Antivirensoftware steht und fällt mit der Aktualität des Programms, insbesondere der Virendefinitionsdatei und der Scan-Engine. Zur Durchführung von regelmäßigen Aktualisierungen ist die Komponente **Geplante Updates** in Ihr Avira Produkt integriert. **Geplante Updates** stellt sicher, dass Avira Mac Security immer aktuell ist und Sie auch vor täglich neu auftauchenden Viren schützt. Das Standardintervall für Updates beträgt 2 Stunden.
Wählen Sie *Planer* > *Update* > *Geplante Updates* > *Ein*.

Hinweis
Es wird dringend davon abgeraten, die standardmäßig aktivierte Option **Geplante Updates** zu deaktivieren.

5. Quarantäne und Logs

5.1 Quarantäne

Erkannte Viren, Malware oder unerwünschte Programme werden im Quarantäneverzeichnis gespeichert. Es ist nicht möglich, Dateien manuell in das Quarantäneverzeichnis zu kopieren. Eine in den Quarantänebereich verschobene Datei kann nicht ausgeführt werden.

Wenn sich eine oder mehrere infizierte Dateien in der Quarantäne befinden, haben Sie verschiedene Optionen zur Verfügung, wie mit diesen umgegangen werden soll.

Im Menü **Aktion für ausgewählte Elemente** können Sie die folgenden Aktionen auswählen:

- **Löschen**: Die infizierte Datei wird unwiderruflich gelöscht.

- **Erneut prüfen**: Die infizierte Datei wird erneut vom **Echtzeit Scanner** geprüft. Eine Datei sollte erneut geprüft werden, wenn die Virendefinitionsdatei Ihres Avira Produkts aktualisiert wurde und Sie einen Fehlalarm vermuten. Wenn der Fehlalarm durch die erneute Prüfung bestätigt wird, können Sie die Datei wiederherstellen. Andernfalls bleibt sie in Quarantäne. Wurde dagegen ein Virus erkannt, wird ein Dialogfenster mit einer *Antivirus-Warnung* angezeigt, das weitere Informationen enthält.

- **Wiederherstellen**: Die erkannte Malware wird im ursprünglichen Ordner wiederhergestellt (sofern dieser noch existiert).

- **Datei an Avira senden**: Sie können Dateien an Avira senden, um sie weiter untersuchen zu lassen. Der Pfad der Datei, die gesendet werden soll, wird automatisch in die Betreffzeile des Sendeformulars eingetragen. Tragen Sie Ihre persönlichen Daten (Name, Email-Adresse) in das Formular ein, und wählen Sie im Menü eine Option aus, die Ihrer Vermutung entspricht. Vergessen Sie nicht, ein Dateiformat für die Antwort-Email von Avira anzugeben. Klicken Sie auf **Hochladen**, um die Datei zu senden. Die Fortschrittsanzeige zeigt den Vorgang des Hochladens an. Die gesendete Datei bleibt in Quarantäne.

Sie können die folgenden Schritte für alle obigen Aktionen anwenden:

- Klicken Sie auf **Anwenden**, um die ausgewählte Aktion durchzuführen.
  Sie werden aufgefordert, Ihr Passwort einzugeben, damit Avira die ausgewählte Aktion durchführen kann.

- Um allen Dateien in Quarantäne eine bestimmte Aktion zuzuweisen, klicken Sie auf **Alle auswählen**. Jede Aktion wird in die Ereignisdatenbank geschrieben und im Bereich der Registerkarte **Logs** des Fensters **Quarantäne & Logs** angezeigt.

- Klicken Sie auf **Erneut laden**, um den Quarantänemanager zu aktualisieren.
  Jede seit der letzten Aktualisierung gefundene Malware wird der Tabelle des Quarantänemanagers hinzugefügt.
  Jede Malware in Quarantäne, der die Aktion **Löschen** oder **Wiederherstellen** zugeordnet ist, wird aus der Tabelle des Quarantänemanagers gelöscht.

5.2 Logs

Sämtliche Informationen der verschiedenen Module von Avira Mac Security werden auf der Registerkarte **Logs** des Fensters **Quarantäne & Logs** angezeigt.
Alle relevanten Ereignisse, wie z. B. Updates, Upgrades, Prüfläufe, Erkennungsergebnisse, Quarantäneverzeichnis, Status der Module und Produktfehler, werden in der Ereignisdatenbank Logs erfasst.

Es ist ratsam, die Größe der Ereignis-Datenbank zu verkleinern, indem man den Zeitrahmen begrenzt, der definiert, wie lange diese Ereignisse aufgezeichnet werden.

Klicken Sie auf der Avira Menüleiste auf *Avira* > *Einstellungen...*. Innerhalb der Kategorie *Allgemein* wählen Sie dann das Register **Logs**.
Hier können Sie einen Zeitrahmen von 1 bis 12 Monaten für aufgezeichnete Logs in der Ereignisdatenbank festlegen.

Hinweis
Als Systemadministrator können Sie die Logdatei des Systems über das Terminal aufrufen:
`/var/log/system.log`

Mehr Informationen über die verschiedenen Einstellungen und für detaillierte Beschreibungen der Funktionen finden Sie im Handbuch der Avira Mac Security. Dieses und aktuelle Informationen finden Sie im Supportbereich der Avira Webseite.

Dieses Handbuch wurde mit äußerster Sorgfalt erstellt. Dennoch sind Fehler in Form und Inhalt nicht ausgeschlossen. Die Vervielfältigung dieser Publikation oder von Teilen dieser Publikation in jeglicher Form ist ohne vorherige schriftliche Genehmigung durch die Avira Operations GmbH & Co. KG nicht gestattet.

Ausgabe Q2-2012

Hier verwendete Marken- und Produktnamen sind Warenzeichen oder eingetragene Warenzeichen ihrer entsprechenden Besitzer. Geschützte Warenzeichen sind in diesem Handbuch nicht als solche gekennzeichnet. Dies bedeutet jedoch nicht, dass sie frei verwendet werden dürfen.

AVIRA

live free.™

© 2012 Avira Operations GmbH & Co. KG. Alle Rechte vorbehalten.
Irrtümer und technische Änderungen vorbehalten.

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
88069 Tettnang
Germany

Telefon: +49 7542-500 0
Telefax: +49 7542-500 3000
www.avira.de